

USE OF SOCIAL MEDIA POLICY

PURPOSE

The purpose of the North Carolina Information Sharing and Analysis (NCISAAC) Use of Social Media Policy¹ is to establish guidelines for the use of social media in crime analysis, situational assessments/awareness, criminal intelligence development and in the support of criminal investigations. This policy defines a minimum set of guidelines which govern the use of Social Media technologies and has been established for the purpose of protecting individual's privacy, civil rights, and civil liberties and to ensure that the Social Media tool is used appropriately.

SOCIAL MEDIA TECHNOLOGIES

To support authorized local, state, federal and tribal law enforcement and public safety agencies, the NCISAAC utilizes Social Media technologies, and supporting software, to gather and analyze information of legitimate interest to law enforcement. Social Media technologies refer to the means of interactions among people in which they create, share, and/or exchange information and ideas in virtual communities and networks utilizing the technological foundations that allow the creation and exchange of user-generated content.

UTILIZATION OF SOCIAL MEDIA

- A. Social media may be used by NCISAAC personnel for the following law enforcement/public safety purposes.
 1. Crime analysis;
 2. Situational assessment/awareness;
 3. Developing criminal intelligence; or
 4. Supporting criminal investigations
- B. While on-duty NCISAAC personnel will utilize social media, access social media websites, use online aliases, and social media monitoring tools only for a valid law enforcement/public safety purpose.
- C. NCISAAC personnel will only utilize social media to seek or retain information that:
 1. Is based upon a criminal predicate, threat to public safety; or

¹ This policy is consistent with and partially draws from the February 2013 US DOJ Global Justice Information Sharing Initiative (GLOBAL) guidance entitled Developing a Policy on the Use of Social Media in Intelligence and

is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense, or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation and the information is relevant to the criminal conduct.

D. NCISAAC personnel will not utilize social media to seek or retain information about:

1. Individuals or organizations solely on the basis of their religious, political, social views or activities;
2. An individual's participation in a particular non-criminal organization or lawful event;
3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual; or
4. An individual's age other than to determine if someone is a minor.
5. To collect information on an individual for personal reasons or gain.

E. NCISAAC personnel will not directly or indirectly receive, seek, accept, or retain information from:

1. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or
2. A source that used means to gather the information which may be prohibited by either law or policy.

AUTHORIZATION TO ACCESS SOCIAL MEDIA WEBSITES

This section addresses the authorization necessary to utilize social media and access social media websites for crime analysis, situational assessments and awareness, developing criminal intelligence and supporting criminal investigations.

A. Public Domain

No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.

B. Online Alias

An online alias may only be used to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense, or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation and the information is relevant to the criminal conduct; and
2. Is related to crime analysis, situational assessments/awareness, developing criminal intelligence, or supporting a criminal investigation.

C. Authorization for Online Aliases

Online Alias – Is defined as an identity encompassing identifiers, such as name and date of birth, differing from the individual user's actual identifiers that is communicated through the use of a nongovernmental Internet Protocol (IP) address. An online alias may **only** be used to **monitor** activity on social media websites. Without prior authorization, personnel are prohibited from using an online alias for undercover activity, which is defined as engaging and interacting with others online. For authorization to use an online alias for **an undercover purpose**, refer to Section IV (D).

1. To receive authorization to use an online alias, NCISAAC personnel shall submit an online alias memorandum to their immediate supervisor.
2. The memorandum must contain the following information:
 - a. An explanation of the valid law enforcement and/or public safety purpose for the request;
 - b. Username/Login information. (Do not include the password(s) for online aliases and ensure that the password(s) are secure at all times);
 - c. List of social media platform(s) to be accessed; and
 - d. Any Identity and/or background information to be utilized for the online alias, to include but not be limited to; email address(es), physical addresses, date of birth, employment, special interests, personal or professional affiliations, and any photographs or images to be used, or any other background

information that is anticipated to be required as part of the process to establish the online alias.

3. The immediate supervisor shall evaluate the request to determine whether an online alias would serve a valid law enforcement or public safety purpose. If determined to meet the standards as outlined by this policy, the immediate supervisor will forward the online aliases request via the chain of command to the Assistant Special Agent in Charge for final review. Unless otherwise delegated, the Assistant Special Agent in Charge shall approve or deny the request and will notify the immediate supervisor of his/her decision. The approved or denied online alias request form will be returned to the immediate supervisor where it will be uploaded and retained on the NCISAAC share drive.
4. All online alias requests will be retained for a period of two years from the date of deactivation or denial. It shall be the responsibility of the immediate supervisor to update the status of the online alias on the NCISAAC share drive if it has been deactivated. NCISAAC personnel are also responsible for notifying their immediate supervisor if they have deactivated their approved online alias.
5. If NCISAAC personnel are asked to assume an undercover alias as created by a law enforcement partner and monitor online activity, for the purpose of furthering a criminal investigation or collection of criminal intelligence, the NCISAAC personnel will be required to obtain authorization to utilize the online alias in compliance with this policy.
6. NCISAAC personnel with an approved online alias may use their online alias to make false representations in concealment of personal identity in order to establish social media accounts (i.e. a twitter account, Facebook). However, NCISAAC personnel are prohibited from using an online alias for undercover activity unless authorized in accordance with the provisions set forth in Section IV (D). The establishment of a social media account with an approved online alias must be documented and submitted to their immediate supervisor.

D. Authorization for use of Online Alias for Undercover Activity

Online Undercover Activity— Is defined as the utilization of an online alias to **engage** in interactions with a person via social media sites that may or may not be in the public domain (i.e. “friending a person on Facebook”).

1. NCISAAC personnel who have an authorized online alias may also request authorization to engage in online undercover activity.
2. Online undercover activity occurs when the NCISAAC personnel utilizing the online alias interacts with a person via social media. Online undercover operations will only be utilized when there is reason to believe that criminal offenses have been, will be or are being committed (e.g. internet chat rooms where child exploitation occurs).
3. Personnel must submit an Online Undercover Activity memorandum to engage in online undercover activity. The request must contain the following information:
 - a. Online alias(es) to be used in the online undercover activity;
 - b. Social media accounts utilized;
 - c. Law enforcement agency being supported;
 - d. Law enforcement agency's case number;
 - e. Valid law enforcement purpose; and
 - f. Anticipated duration for the online undercover activity.
4. The immediate supervisor shall evaluate the request to determine whether online undercover activity meets the requirements as set forth in this policy. If determined to meet the necessary standards, the immediate supervisor shall forward the request for online undercover activity via the chain of command to the Special Agent in Charge or his/her designee. Unless otherwise delegated, the SAC or designee shall approve or deny the request and will notify the immediate supervisor of his or her decision. The original approved or denied online undercover activity request form will be returned to the immediate supervisor where it will be uploaded and retained on the NCISAAC share drive. All online undercover activity requests will be retained for a period of two years from the date of deactivation or denial. It shall be the responsibility of the immediate supervisor to notify the SAC or his/her designee via the chain of command when an online undercover request has been deactivated.
5. In situations involving exigent circumstances, the unit supervisor may obtain via the chain of command verbal authorization for online undercover activity. The unit supervisor shall provide written documentation of the request, to include the exigent circumstances, and the circumstances of the verbal authorization as soon as practical.
6. If NCISAAC personnel are asked to assume an undercover alias as created by a law enforcement partner and conduct online undercover activity, for the purpose of furthering a criminal investigation or collection of criminal intelligence, the NCISAAC

personnel will be required to obtain authorization to utilize the online alias in undercover activity in compliance with this policy.

7. Once authorized to engage in online undercover activity, the NCISAAC personnel shall utilize the appropriate de-confliction system.
8. A record will be maintained of **all** online undercover activity to include chat transcriptions, interaction logs, etc.
9. All approved online undercover activity requests will be reviewed weekly by the immediate supervisor to ensure continued need for the online undercover activity. Approved online undercover activity that does not provide pertinent information related to a valid law enforcement purpose within thirty (30) days, will be discontinued.
10. A summary of the online undercover activity, to include the date of termination will be placed in the intelligence file by NCISAAC personnel authorized to use the online alias. The online alias, with supervisor authorization, may be maintained if it is anticipated that it will be utilized again.

AUTHORIZATION TO UTILIZE SOCIAL MEDIA MONITORING TOOLS

- A. The **Social Media Monitoring Tool** may be utilized in criminal investigations; criminal intelligence development; crime analysis; and situational assessments/awareness (e.g. sporting and community events) without written approval and on an as-needed basis. Supervisors shall be responsible for the day-to-day usage of the social media monitoring tool by members under their chain-of-command.
- B. Prior to utilizing a social media monitoring tool for any First Amendment-related activity (e.g. during demonstrations or other large gatherings that require a law enforcement presence to ensure the safety of the public), the unit supervisor will submit a written request through the chain of command to the Special Agent in Charge (SAC) of NC ISAAC for authorization to use the social media monitoring tool. The request must contain the following:
 1. A description of the social media monitoring tool;
 2. Its purpose and intended use;
 3. The social media websites the tool will access;
 4. Whether the tool is accessing information in the public domain or information protected by privacy settings; and

5. Whether information will be retained by the NCISAAC and if so, the applicable retention period for such information.
6. The written request/approval or denial by the SAC or his/her designee will be uploaded and retained on the NCISAAC share drive.

C. In exigent circumstances relating to First Amendment activity, the unit supervisor may obtain verbal authorization via the chain of command to utilize the social media monitoring tool and provide written documentation as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.

The continued use of the social media monitoring tool will be reviewed annually by the Unit's supervising Deputy Director to determine if the social media monitoring tool still serves a valid Law Enforcement/public safety purpose.

DOCUMENTATION AND RETENTION

Crime analysis and situational assessments may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the special event or situation requiring the report or First Amendment-protected event where there was no criminal activity related to the information gathered, the information obtained from the social media monitoring tool will be retained for no more than fourteen (14) days. Information from the social media monitoring tool that does indicate a criminal nexus will be retained in a suspicious activity report, or intelligence report.

Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes.

OFF DUTY CONDUCT

NCISAAC personnel will not utilize approved online aliases, approved undercover accounts or activity, or approved social media monitoring tools for personal use.

PERSONAL EQUIPMENT AND PERSONAL SOCIAL MEDIA WEBSITES AND PASSWORDS

Given the ease with which information can be gathered from public internet searches, tracking services, and other computer analytic technology, the use of personal social media websites are not allowed; however, the use of personal or family internet accounts to include wireless internet service connections is allowed when conducting investigations and being used for NC ISAAC official use or business related matters.

RETENTION AND DISSEMINATION

Retention and dissemination of social media information will be treated in the same manner as intelligence contained in the NCISAAC Intelligence Management System. Information developed during the course of a criminal investigation and provided to the agency responsible for the criminal investigation, shall retain all NCISAAC work product relative to the criminal investigation. The responsible investigating agency will be responsible for the maintenance, dissemination, and destruction of the criminal investigation pursuant to state and federal laws.

COMPLAINTS AND EMPLOYEE MISCONDUCT

Personnel will report violations or suspected violations of this directive to their immediate supervisor in accordance with the NCISAAC Privacy Policy.

Complaints from the public regarding information obtained from social media websites will be submitted to their direct supervisor and handled in accordance with the NCISAAC Privacy Policy and the SBI policy and procedures. **If the information is determined to be erroneous, the information will be corrected or deleted.**

AUDIT

As part of the NCISAAC annual privacy audit, compliance with this directive will be verified by a NCISAAC inspection team led by the SBI. Audit results shall be reported in writing and will be included as part of the annual privacy audit report.

Audit will consist of the following;

1. Review of all approved “Online Alias” Requests

2. Review of all approved “Online Alias for Undercover Activity” Requests
3. Review of all approved “Social Media Monitoring Tools” written requests
4. A sampling of authorized Social Media Accounts from the prior 12 month period to verify proper use in accordance with the above authorized uses

ANNUAL REVIEW

The NCISAAC Social Media Policy will be reviewed, and updated as necessary, no less frequently than every 12 months. Changes in data sources, technology, data use and/or sharing agreements, and other relevant considerations. This policy review will be verified by the NC ISAAC Privacy Officer and the NC ISAAC Special Agent in Charge.

TRAINING

Only NCISAAC personnel trained in the use of Social Media technologies, including its privacy and civil liberties protections, shall be allowed to use social media technologies. Training shall occur no less frequently than every 12 months and consist of:

1. Legal authorities, developments, and issues involving the use of Social Media technologies;
2. Current NC ISAAC Policy regarding appropriate use of Social Media;
3. Evolution of Social Media technologies, including new capabilities and associated risks;
4. Technical, physical, administrative, and procedural measures to protect the security of Social Media technologies against unauthorized access or use;
5. Practical exercises in the use of the NCISAAC Social Media monitoring system; and
6. Techniques, processes and requirements to verify the validity of information obtained through social media resources.

Training shall be updated as technological, legal, and other changes that affect the NCISAAC Use of Social Media Policy occur and will be provided to NCISAAC personnel no less than one time per calendar year.

ELECTRONIC SECURITY OF SOCIAL MEDIA INFORMATION:

Information collected by NCISAAC personnel through the use of Social Media will be stored in a secured law enforcement database.

Access to the information is limited to law enforcement staff in good standing who have completed law enforcement background investigations.

NCISAAC will utilize strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system.

SANCTIONS FOR MISUSE

NCISAAC personnel who violate the provisions of this directive will be subject to disciplinary action, up to and including termination.

Definitions

Crime Analysis and Situational Assessment/Awareness—Analytic activities to enable NCHIDTA/NCRIC to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

Criminal Intelligence Information—Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

Criminal Nexus—Established when behavior or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity or enterprise.

Online Alias—An online identity encompassing identifiers, such as name and date of birth, differing from the individual's actual identifiers, that uses a nongovernmental Internet Protocol (IP) address. Online alias may be used to monitor activity on social media websites or to engage in authorized online undercover activity.

Online Undercover Activity—The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain (i.e. "friending a person on Facebook").

Public Domain—Any Internet resource that is open and available to any person.

Social Media—A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social media networking sites (Facebook, MySpace), micro blogging sites (Twitter), p

Social Media Monitoring Tool—A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include BlueJay, Snaptrends, Netbase, Twitterfall, Trackur, Tweetdeck, Socialmention, Socialpointer, and Plancast.

Social Media Websites—Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), micro blogging sites (Twitter, Nixle), photo-and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.